

# Simulating Concordant Computations

Bryan Eastin\*

*National Institute of Standards and Technology, Boulder, CO 80305*

A quantum state is called concordant if it has zero quantum discord with respect to any part. By extension, a concordant computation is one such that the state of the computer, at each time step, is concordant. In this paper, I describe a classical algorithm that, given a product state as input, permits the efficient simulation of any concordant quantum computation having a conventional form and composed of gates acting on two or fewer qubits. This shows that such a quantum computation must generate quantum discord if it is to efficiently solve a problem that requires super-polynomial time classically. While I employ the restriction to two-qubit gates sparingly, a crucial component of the simulation algorithm appears not to be extensible to gates acting on higher-dimensional systems.

The search for the origin of the computational power of quantum mechanics has proven to be a recurring theme in quantum information theory. Primarily, this search has focused on identifying the feature of quantum mechanics that permits the efficient<sup>1</sup> solution of certain classically intractable problems. In addition to being useful, computational speedups of this magnitude are intriguing since, classically, no such improvement is to be found over rather basic models of computation, e.g., the Turing machine.

Among the proposed sources of this quantum advantage, the most widely studied is a kind of non-local correlation known as entanglement [1]. The state of a composite system is entangled if it cannot be described in terms of a, possibly uncertain, local assignment of states to individual subsystems. Classically, non-trivial correlations indicate imperfect information about the state of the system, but entanglement is possible for quantum states of maximal knowledge, or pure states. At the extreme, an entangled state of a composite system may be pure while the marginal state of the component subsystems is maximally impure, or maximally mixed. In other words, one may know everything possible about the state of a composite quantum system without knowing anything about the state of the component subsystems. As a distinctly non-classical property and a necessary resource for protocols such as teleportation and quantum error correction, entanglement is a natural suspect when investigating the power of quantum computing.

There are two kinds of evidence in favor of entanglement as the crucial resource for achieving speedups that enable the efficient solution of a classically intractable problem, a variety of speedup henceforth labeled Promethean. First, there are proofs that pure-state quantum computations generating only limited amounts of entanglement can be efficiently simulated classically and are therefore incapable of solving any problem that

cannot be solved in polynomial time by a classical computer. An early result of this sort was shown by Jozsa and Linden [2], who described a method for efficiently simulating any quantum computation whose correlations are approximately confined to regions of bounded size. Shortly thereafter, Vidal proposed an efficient simulation algorithm for quantum computations whose maximum Schmidt rank for any bipartition of the computer scales at most as a polynomial [3]. These methods of simulation can each be applied to quantum computations with either mixed or pure states, but in the former case classical correlations, in addition to entanglement, are restricted. The second kind of evidence for the importance of entanglement is its apparent generation by all implementations of Shor's quantum factoring algorithm. In particular, a typical implementation of Shor's algorithm has been shown to generate entanglement that precludes its simulation by either Jozsa and Linden's or Vidal's method [2, 4]. To summarize, entanglement is necessary for obtaining Promethean speedups with pure-state quantum computing, and there are indications that it may be required for Shor's algorithm.

Regarding mixed states, further, and contrary, evidence comes from the DQC1 model of quantum computation [5], where all but one of the qubits in the computer is initially prepared in the maximally mixed state. DQC1 is believed to be strictly less powerful than pure-state quantum computing [5, 6], but it nonetheless seems to be capable of providing Promethean speedups in, for example, trace estimation. Datta, Flammia, and Caves have shown numerically that trace estimation is possible even with a vanishing amount of entanglement (as measured by the negativity of bipartite splittings) [7]. Nevertheless, Datta and Vidal have shown that the Schmidt rank grows exponentially for certain bipartitions of a quantum computer performing trace estimation [8], thereby demonstrating the existence of correlations, though not necessarily entanglement, sufficient to thwart Vidal's simulation method. Based on these results, it seems probable that Promethean speedups are possible even in the absence of entanglement.

But if entanglement is not the source of Promethean speedups in DQC1 then we are left to ask what is. Among the proposed alternatives is a measure of non-classical

---

\*Electronic address: [beastin@nist.gov](mailto:beastin@nist.gov)

<sup>1</sup> The definition of "efficient" is taken from classical computer science, where it refers to any computation that requires an amount of resources (particularly time steps) scaling at most polynomially with the problem size.

correlation known as quantum discord [9]. Datta, Shaji, and Caves have shown that discord is indeed present in the trace-estimation algorithm [10], but it has never been proven to be necessary. The work presented in this paper was motivated by the desire to show that discord is necessary for Promethean speedups in mixed-state quantum computations. Since, for pure states, discord reduces to a measure of entanglement, this would amount to an extension of the result (described above) about the utility of entanglement in pure-state quantum computing. To this end, I considered the difficulty of simulating concordant computations, i.e., those that generate no quantum discord, as suggested by Ref. [11].

Here, I describe an algorithm for efficiently simulating, using a classical computer, any computation that does not generate discord and consists of a sequence of one- and two-qubit unitary gates followed by single-qubit measurements. Section I briefly introduces some notation and Sec. II covers discord, concordance, and concordant computations and proves a few results that are employed later. My simulation algorithm is described for quantum computations in a conventional form in Sec. III and extensions to non-conventional forms are discussed in Sec. IV. The conclusion contains a discussion of open problems.

## I. NOTATION

Unitary operators, projectors, and sets are denoted by capital roman letters in math-italic, black-board, and calligraphic font, respectively, e.g.,  $U$ ,  $\mathbb{P}$ , and  $\mathcal{A}$ . For more generic functions on quantum states I use capital Roman letters in math font. Throughout the paper, quantum operators and states are given subscripts (which may be sets) to denote the subsystems they act upon and/or to index the component corresponding to that subsystem; all other identifying indices and labels are represented as superscripts. Thus, the state of a composite system can be expressed as  $\rho_{AB}$ , where  $\mathcal{A}$  and  $\mathcal{B}$  are disjoint sets indexing the subsystems, and the marginal density operator of part  $\mathcal{B}$  of  $\rho_{AB}$  is written as  $\rho_{\mathcal{B}} = \text{tr}_{\mathcal{A}}(\rho_{AB})$ , where  $\text{tr}_{\mathcal{A}}$  is the trace over part  $\mathcal{A}$ . Contrary to this example, I frequently omit the subscript when it would specify the entire system. Whenever indicated, the time step is labeled by a superscript. The symbols  $\cup$ ,  $\cap$ ,  $\setminus$ , and  $\ominus$  are used to denote the set-theoretic operations of union, intersection, difference, and symmetric difference, and  $\bar{\mathcal{G}}$  denote the complement of a set  $\mathcal{G}$  by  $\bar{\mathcal{G}}$ . Vectors over finite fields are denoted by placing a right arrow over a symbol, and the subscripting of such vectors by a set represents the restriction of the vector to the components indicated by the set, e.g.,  $\vec{i}_{\mathcal{G}} = \{i_k : k \in \mathcal{G}\}$ . The support of an operator is taken to mean the set of subsystems upon which the operator acts nontrivially.

## II. CONCORDANCE

The notion of a classical state frequently carries with it the idea of a preferred basis. In a Stern-Gerlach experiment, for example, the resulting superposition of different spins and locations is rarely considered as simply representing a novel basis for classical particles. From this perspective, a classical state is one selected from a preferred basis of orthogonal states, where the basis for a composite system arises from the tensor product of the preferred bases for the component subsystems. When the state of a system is uncertain, we describe it using a probability distribution over known, or pure, classical states.

A concordant state differs from this definition of classicality only in that no preferred basis is specified; any set of orthogonal bases for the subsystems may be used to determine the pure states allowed to the composite system. I take a concordant computation, in turn, to be one in which the state of the computer after any step is concordant. This usage of “concordant” seems to have been coined by Andrew White, but it has not previously appeared in publication. In the following subsections, I explicitly define concordant states and computations as well as reviewing or proving some results used later in the paper.

### A. Quantum discord

Quantum discord is a measure of non-classical correlations introduced by Zurek [9]. Intuitively, it quantifies the amount of non-local disturbance caused by measuring part of a quantum state. For a quantum state  $\rho_{AB}$ , the quantum discord with respect to part  $\mathcal{B}$  can be defined as

$$D_{\mathcal{B}}(\rho_{AB}) = \min_{\{\mathbb{P}_{\mathcal{B}}^i\}} \left[ H(\rho_{AB}^{\{\mathbb{P}_{\mathcal{B}}^i\}}) - H(\rho_{\mathcal{B}}^{\{\mathbb{P}_{\mathcal{B}}^i\}}) \right] - [H(\rho_{AB}) - H(\rho_{\mathcal{B}})]$$

where  $\{\mathbb{P}_{\mathcal{B}}^i\}$  is a complete set of orthogonal one-dimensional projectors (CSOOP) on part  $\mathcal{B}$ ,

$$\rho_{AB}^{\{\mathbb{P}_{\mathcal{B}}^i\}} = \sum_i \mathbb{P}_{\mathcal{B}}^i \rho_{AB} \mathbb{P}_{\mathcal{B}}^i,$$

and  $H(\rho) = -\text{tr}(\rho \log_2 \rho)$  is the Von Neumann entropy, the quantum analog of Shannon entropy. This definition is somewhat less general than that of Zurek, who did not insist on the minimization, instead making quantum discord a function of the choice of projectors.

Ollivier and Zurek [12] showed that  $D_{\mathcal{B}}(\rho_{AB}) = 0$  if and only if

$$\rho_{AB} = \sum_i \mathbb{P}_{\mathcal{B}}^i \rho_{AB} \mathbb{P}_{\mathcal{B}}^i \quad (1)$$

for some CSOOP  $\{\mathbb{P}_{\mathcal{B}}^i\}$  on part  $\mathcal{B}$ , or equivalently,

$$\rho_{AB} = \sum_i \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{P}_{\mathcal{B}}^i) \otimes \mathbb{P}_{\mathcal{B}}^i = \sum_i p_i \rho_{\mathcal{A}}^{\mathbb{P}_{\mathcal{B}}^i} \otimes \mathbb{P}_{\mathcal{B}}^i \quad (2)$$

where  $p_i = \text{tr}(\rho_{AB} \mathbb{P}_{\mathcal{B}}^i)$ ,  $\rho_{\mathcal{A}}^{\mathbb{P}_{\mathcal{B}}^i} = \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{P}_{\mathcal{B}}^i)$ , and

$$\rho_{\mathcal{A}}^{\mathbb{P}_{\mathcal{B}}^i} = \mathbb{P}_{\mathcal{B}}^i \rho_{AB} \mathbb{P}_{\mathcal{B}}^i / \text{tr}(\rho_{AB} \mathbb{P}_{\mathcal{B}}^i). \quad (3)$$

Lemma 1 shows that the set of projectors satisfying Eq. 1 is unique up to degeneracy in part  $\mathcal{B}$  of  $\rho_{AB}$ . The notion of degeneracy on a part of a larger state is clarified by Definition 1.

**Definition 1.** Two states are degenerate on part  $\mathcal{B}$  of  $\rho_{AB}$  if the corresponding projectors  $\mathbb{P}_{\mathcal{B}}$  and  $\mathbb{Q}_{\mathcal{B}}$  satisfy  $\text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{P}_{\mathcal{B}}) = \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{Q}_{\mathcal{B}})$ .

**Lemma 1.** Given two CSOOPs on  $\mathcal{B}$ ,  $\{\mathbb{P}_{\mathcal{B}}^i\}$  and  $\{\mathbb{Q}_{\mathcal{B}}^j\}$ , and a state  $\rho_{AB} = \sum_i \mathbb{P}_{\mathcal{B}}^i \rho_{AB} \mathbb{P}_{\mathcal{B}}^i$ ,  $\rho_{AB} = \sum_j \mathbb{Q}_{\mathcal{B}}^j \rho_{AB} \mathbb{Q}_{\mathcal{B}}^j$  if and only if  $\text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{P}_{\mathcal{B}}^i) = \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{Q}_{\mathcal{B}}^j)$  for all  $\mathbb{P}_{\mathcal{B}}^i \mathbb{Q}_{\mathcal{B}}^j \neq 0$ .

*Proof.* The forward implication follows from

$$\begin{aligned} \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{P}_{\mathcal{B}}^i \mathbb{Q}_{\mathcal{B}}^j) &= \sum_h \text{tr}_{\mathcal{B}}(\mathbb{P}_{\mathcal{B}}^h \rho_{AB} \mathbb{P}_{\mathcal{B}}^h \mathbb{P}_{\mathcal{B}}^i \mathbb{Q}_{\mathcal{B}}^j) \\ &= \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{P}_{\mathcal{B}}^i \mathbb{Q}_{\mathcal{B}}^j \mathbb{P}_{\mathcal{B}}^i) = e_{ij} \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{P}_{\mathcal{B}}^i) \\ &= \sum_h \text{tr}_{\mathcal{B}}(\mathbb{Q}_{\mathcal{B}}^h \rho_{AB} \mathbb{Q}_{\mathcal{B}}^h \mathbb{P}_{\mathcal{B}}^i \mathbb{Q}_{\mathcal{B}}^j) \\ &= \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{Q}_{\mathcal{B}}^j \mathbb{P}_{\mathcal{B}}^i \mathbb{Q}_{\mathcal{B}}^j) = e_{ij} \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{Q}_{\mathcal{B}}^j) \end{aligned}$$

where  $e_{ij} = \text{tr}_{\mathcal{B}}(\mathbb{P}_{\mathcal{B}}^i \mathbb{Q}_{\mathcal{B}}^j)$ . The reverse implication follows from

$$\begin{aligned} \rho_{AB} &= \sum_i \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{P}_{\mathcal{B}}^i) \otimes \mathbb{P}_{\mathcal{B}}^i \\ &= \sum_{i,j} \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{P}_{\mathcal{B}}^i) \otimes (\mathbb{P}_{\mathcal{B}}^i \mathbb{Q}_{\mathcal{B}}^j) \\ &= \sum_{i,j} \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{Q}_{\mathcal{B}}^j) \otimes (\mathbb{P}_{\mathcal{B}}^i \mathbb{Q}_{\mathcal{B}}^j) \\ &= \sum_j \text{tr}_{\mathcal{B}}(\rho_{AB} \mathbb{Q}_{\mathcal{B}}^j) \otimes \mathbb{Q}_{\mathcal{B}}^j. \end{aligned}$$

□

If the quantum discord of  $\rho_{AB}$  is zero with respect to both  $\mathcal{A}$  and  $\mathcal{B}$  then, by two applications of Eq. 1,

$$\rho_{AB} = \sum_{i,j} p_{ij} \mathbb{P}_{\mathcal{A}}^i \otimes \mathbb{P}_{\mathcal{B}}^j \quad (4)$$

for some CSOOPs  $\{\mathbb{P}_{\mathcal{A}}^i\}$  and  $\{\mathbb{P}_{\mathcal{B}}^j\}$ . For fixed  $\{\mathbb{P}_{\mathcal{A}}^i\}$ , Lemma 1 shows that the set of projectors  $\{\mathbb{P}_{\mathcal{B}}^j\}$  satisfying Eq. 4 is unique up to the degeneracy common to all  $\rho_{\mathcal{B}}^{\mathbb{P}_{\mathcal{A}}^i}$ , that is, up to degeneracy appearing in each of the subblocks of  $\rho$  projected out by some  $\mathbb{P}_{\mathcal{A}}^i$ .

## B. Concordant states

The adjective “concordant” is intended to indicate a lack of quantum discord. Because discord is an asymmetric, bipartite measure, however, it is not completely obvious what this restriction ought to mean with regard to quantum states, especially states of composite systems composed of more than two subsystems. I choose to label a state as concordant if it has zero discord with respect to any part. This is codified in the following definition.

**Definition 2.** A state  $\rho$  is concordant if  $D_{\mathcal{A}}(\rho) = 0$  for any strict subset  $\mathcal{A}$  of the subsystems of  $\rho$ .

In particular, Def. 2 guarantees that  $D_k(\rho) = 0$  for any  $k$  labeling a single subsystem of some concordant state  $\rho$ . By Eq. 1, this implies that, for any concordant state  $\rho$ , there exists a CSOOP  $\{\mathbb{P}_k^i\}$  for every subsystem  $k$  such that

$$\rho = \sum_i \mathbb{P}_k^i \rho \mathbb{P}_k^i. \quad (5)$$

An equivalent form of the implication that often proves useful is

$$\rho = \sum_{\vec{i}} \mathbb{P}^{\vec{i}} \rho \mathbb{P}^{\vec{i}} = \sum_{\vec{i}} p_{\vec{i}} \mathbb{P}^{\vec{i}} \quad (6)$$

where  $\mathbb{P}^{\vec{i}} = \prod_k \mathbb{P}_k^{i_k}$  and  $\{\mathbb{P}_k^{i_k}\}$  for fixed  $k$  is a CSOOP for the  $k$ th subsystem.

The reasoning above shows that Def. 2 implies Eq. 6, but conversely, any state satisfying Eq. 6 clearly satisfies Def. 2. Thus, Eq. 6 can be taken as an alternate definition of a concordant state. In words, a state is concordant if there exists a product basis, that is, a basis arising from the tensor product of local orthogonal bases, such that its density operator is diagonal.

## C. Concordant computations

In keeping with standard practice, I adopt a description of quantum computation based on the quantum circuit model, where the evolution of the state of a system is described by a sequence of operators. Most generally, the operations applied can be chosen probabilistically, based, for example, on the path the computation has taken thus far, as revealed by measurements. In this model, it is natural to label a computation as concordant if the state of the computer is concordant both initially and after each step of the evolution, a notion formalized below.

**Definition 3.** A quantum computation described by a sequence of operators  $\{G^t\}$  acting on some input state  $\rho^0$  is concordant if each state  $\rho^t = G^t \circ \dots \circ G^2 \circ G^1(\rho^0)$  is concordant for every path of the computation.

Being concordant, each computational state might be considered classical for some choice of the classical basis, but a concordant computation is slightly more general than a randomized classical computation in that the product eigenbasis can change from one step to the next.

Definition 3 is problematic for questions of computational complexity since it is possible to obscure the difficulty of an algorithm by employing very complex operations or initial states. The specification of an arbitrary input state  $\rho^0$ , for example, entails a quantity of real numbers exponential in the number of subsystems, even if  $\rho^0$  is concordant. (See Ref. [2] for a careful treatment of the difficulties posed by the use of real numbers.) I avoid these problems and simplify the following discussion by initially considering only computations that are conventional, as defined by Def. 4. In Sec. IV I discuss ways in which the restriction to conventional computations can be relaxed.

**Definition 4.** *A conventional quantum computation consists of an input product state diagonal in the standard basis,  $\rho^0 = \bigotimes_k \rho_k^0$ , followed by a sequence of unitary gates  $\{G^t\}$ , and concluded by single-subsystem measurements determining the outcome of the computation. Each  $\rho_k^0$  and  $G^t$  (when restricted to its support) is required to be efficiently computable.*

The evolution of a concordant computation of the form given by Def. 4 is particularly simple. Because the spectrum of a density operator is invariant under conjugation by unitary operators, any unitary gate can be considered simply as a change of eigenbasis for the density operator. For a concordant computation, there is guaranteed to exist a product basis, both before and after a gate, such that the density operator describing the state of the computer is diagonal. Thus, the effect of any unitary operator can be, at most, to change the product eigenbasis and permute the associated eigenvalues.

More specifically, Lemma 2 shows that a transformation between concordant states induced by a unitary gate with support  $\mathcal{G}$  is equivalent to a change of product eigenbasis on  $\mathcal{G}$  together with a permutation with support  $\mathcal{G}$  of the vectors indexing the eigenvalues. In general, the unitary gate will not actually be a permutation followed by a change of product eigenbasis but merely be equivalent to one for the given initial state.

**Lemma 2.** *If  $\sigma = G\rho G^\dagger$  where  $G$  is a unitary operator with support  $\mathcal{G}$ ,  $\rho$  and  $\sigma$  are concordant, and  $\rho = \sum_{\vec{i}} p_{\vec{i}} \mathbb{P}_{\vec{i}}^{\vec{i}}$  then  $\sigma = \sum_{\vec{j}} q_{\vec{j}} \mathbb{P}_{\vec{j}}^{\vec{j}}$  where  $q_{P \cdot \vec{i}} = p_{\vec{i}}$  for some permutation  $P$  with support  $\mathcal{G}$ .*

*Proof.*

Since  $\sigma$  is concordant there exists  $\{\mathbb{Q}_{\vec{j}}^{\vec{j}}\}$  such that

$$\sigma = \sum_{\vec{j} \in \mathcal{G}} \mathbb{Q}_{\vec{j}}^{\vec{j}} \sigma \mathbb{Q}_{\vec{j}}^{\vec{j}},$$

where  $\mathbb{Q}_{\vec{j}}^{\vec{j}} = \prod_{k \in \mathcal{G}} \mathbb{Q}_k^{j_k}$  and likewise for subsequent simi-

lar projectors. Moreover,

$$\begin{aligned} \sum_{\vec{i} \in \mathcal{G}} \mathbb{P}_{\vec{i}}^{\vec{i}} \sigma \mathbb{P}_{\vec{i}}^{\vec{i}} &= \sum_{\vec{i} \in \mathcal{G}} \mathbb{P}_{\vec{i}}^{\vec{i}} G \rho G^\dagger \mathbb{P}_{\vec{i}}^{\vec{i}} \\ &= G \sum_{\vec{i} \in \mathcal{G}} \mathbb{P}_{\vec{i}}^{\vec{i}} \rho \mathbb{P}_{\vec{i}}^{\vec{i}} G^\dagger = G \rho G^\dagger = \sigma. \end{aligned}$$

Thus,  $\sigma$  can be written in the form

$$\sigma = \sum_{\vec{j}} \mathbb{P}_{\vec{j}}^{\vec{j}} \mathbb{Q}_{\vec{j}}^{\vec{j}} \sigma \mathbb{Q}_{\vec{j}}^{\vec{j}} \mathbb{P}_{\vec{j}}^{\vec{j}} = \sum_{\vec{j}} q_{\vec{j}} \mathbb{P}_{\vec{j}}^{\vec{j}} \mathbb{Q}_{\vec{j}}^{\vec{j}}.$$

To see that the specified permutation exists, consider a graph  $\Gamma$  where the nodes correspond to the projectors  $\mathbb{Q}_{\vec{j}}^{\vec{j}}$  and  $G \mathbb{P}_{\vec{i}}^{\vec{i}} G^\dagger$  and two nodes are connected if their associated projectors are not orthogonal. Since  $\{\mathbb{Q}_{\vec{j}}^{\vec{j}}\}$  and  $\{G \mathbb{P}_{\vec{i}}^{\vec{i}} G^\dagger\}$  project onto two eigenbases for the state

$$\sigma_{\mathcal{G}}^{\mathbb{P}_{\vec{i}}^{\vec{i}}} \propto \sum_{\vec{j} \in \mathcal{G}} q_{\vec{j}} \mathbb{Q}_{\vec{j}}^{\vec{j}} = \sum_{\vec{j} \in \mathcal{G}} p_{\vec{j}} G \mathbb{P}_{\vec{j}}^{\vec{j}} G^\dagger,$$

projectors connected in  $\Gamma$  are associated, by the uniqueness properties of the spectral decomposition, with the same eigenvalue of  $\sigma_{\mathcal{G}}^{\mathbb{P}_{\vec{i}}^{\vec{i}}}$  and therefore with the same eigenvalues of  $\sigma$ . Two spectral decompositions of the same density operator are related by a unitary transformation, so each connected component of  $\Gamma$  includes an equal number of projectors from  $\{\mathbb{Q}_{\vec{j}}^{\vec{j}}\}$  and  $\{G \mathbb{P}_{\vec{i}}^{\vec{i}} G^\dagger\}$ . Thus, it is possible to assign  $q_{\vec{j}} = p_{\vec{i}}$  where  $\vec{j} = P \cdot \vec{i}$ ,  $P$  is a permutation such that  $\vec{j}_{\mathcal{G}} = \vec{i}_{\mathcal{G}}$ , and  $\{\mathbb{Q}_{\vec{j}}^{\vec{j}}\}$  and  $\{G \mathbb{P}_{\vec{i}}^{\vec{i}} G^\dagger\}$  are in the same connected component of  $\Gamma$ .  $\square$

### III. SIMULATING A CONVENTIONAL CONCORDANT COMPUTATION

In the previous section I show that the transformation of one concordant state to another by a unitary operator with support  $\mathcal{G}$  is equivalent to a permutation of eigenvalues together with a change of product eigenbasis on  $\mathcal{G}$ . Combined with the fact that a density operator can be considered as a probabilistic mixture of its eigenstates, this suggests the following strategy for simulating a conventional concordant computation: Find a change of product eigenbasis and permutation of the vectors labeling eigenstates (and, therefore, the associated eigenvalues) equivalent to each unitary gate in the computation, and then generate an output of the computation by appropriately picking a vector labeling an eigenstate of the input state, applying the derived permutations to the chosen vector, and evaluating the final measurement on the indicated product state.

It is not immediately obvious that the described simulation is feasible because the permutation and change of



```

01 For each subsystem  $k$ :
02     Choose  $i_k$  according to the probability distribution  $\Pr[i_k = w] = \langle w | U_k^{0\dagger} \rho_k^0 U_k^0 | w \rangle$ .
03      $\vec{j} := P \cdot \vec{i}$ 
04 For each measured subsystem  $k$ :
05     Choose  $h_k$  according to the probability distribution  $\Pr[h_k = w] = |\langle w | U_k^s | j_k \rangle|^2$ .
06 Output  $\vec{h}$ .

```

FIG. 1: Pseudocode for simulating a conventional concordant computation.  $U^0$  and  $U^s$  are unitary product operators identifying the initial and final product eigenbases respectively and  $P$  is the permutation that acts on  $\rho^0$  equivalently to the specified sequence of unitary operators. Pseudocode for converting a sequence of two-qubit unitary operators in a concordant computation into an equivalent classical permutation and change of basis is given in Fig. 2.

eigenbasis equivalent to each unitary operator is dependent on the overall state of the computer. Nonetheless, the following subsections provide detailed descriptions of the necessary subcomponents of such a simulation for the special case of two-qubit unitary gates, thereby proving Theorem 1. Section III A shows how a conventional concordant computation can be simulated given the permutation and eigenbasis change equivalent to each unitary operator. Section III B proves that it is possible to efficiently determine a permutation and change of eigenbasis equivalent to a unitary operator from the degeneracy of the pre-gate state. Finally, Sec. III C explains how the relevant degeneracy can be found from the previously applied permutations and an input product state, so long as the computation contains only one- and two-qubit unitary gates. In addition to the concordant-state condition given by Eq. 6, I employ an equivalent definition: a state  $\rho$  is concordant if and only if there exists a unitary product operator  $U = \bigotimes_k U_k$  such that  $U^\dagger \rho U$  is diagonal in the standard basis.

**Theorem 1.** *A conventional concordant computation with unitary operators having support on only one or two qubits can be efficiently simulated by a classical computer.*

### A. Simulation given many hints

Consider a conventional concordant computation for which the sequence of unitary operators employed,  $\{G^t\}$ , is known to act equivalently to the sequence  $\{U^t P^t U^{t-1\dagger}\}$  where each  $P^t$  is a permutation (that is, a classical reversible gate) with the same support as  $G^t$  and each  $U^t$  is a unitary product operator that transforms from the standard basis to the product eigenbasis at time step  $t$ . Given this information, the initial state  $\rho^0$  must be of the form

$$\rho^0 = \sum_{\vec{i}} p_i^0 U^0 |\vec{i}\rangle \langle \vec{i}| U^{0\dagger} \quad (7)$$

where each  $|\vec{i}\rangle$  is an element of the standard basis. (By definition,  $U^0$  is trivial for a conventional computation.)

The state of the computer after one step of the computation is

$$\begin{aligned} \rho^1 &= \sum_{\vec{i}} p_i^0 G^1 U^0 |\vec{i}\rangle \langle \vec{i}| U^{0\dagger} G^{1\dagger} \\ &= \sum_{\vec{i}} p_i^0 U^1 U^{1\dagger} G^1 U^0 |\vec{i}\rangle \langle \vec{i}| U^{0\dagger} G^{1\dagger} U^1 U^{1\dagger} \\ &= \sum_{\vec{i}} p_i^0 U^1 P^1 |\vec{i}\rangle \langle \vec{i}| P^{1\dagger} U^{1\dagger} \end{aligned}$$

where  $P^1$  is a permutation that acts identically to  $U^{1\dagger} G^1 U^0$  on  $U^{0\dagger} \rho^0 U^0$ . Iterating this process yields

$$\rho^s = \sum_{\vec{i}} p_i^0 U^s \left( \prod_{t=s}^1 P^t \right) |\vec{i}\rangle \langle \vec{i}| \left( \prod_{t=1}^s P^{t\dagger} \right) U^{s\dagger} \quad (8)$$

where each  $P^t$  is a permutation that acts identically to  $U^{t\dagger} G^t U^{t-1}$  on  $U^{t-1\dagger} \rho^{t-1} U^{t-1}$ .

The measurement statistics of a mixed state are identical to those of a probabilistically chosen state in its decomposition where the probability is given by the coefficient of the term associated with that state. Thus, the expression for the final pre-measurement state shown in Eq. 8 suggests the following simple technique for simulating the computation: Choose a single vector  $\vec{i}$  according to the probability distribution  $p_i^0$ , which can be done efficiently since  $\rho^0$  is a product state. Apply the permutation  $\prod_{t=s}^1 P^t$  to  $\vec{i}$  to obtain a new vector  $\vec{j}$  identifying one component of the final pre-measurement state. And last, for each measured subsystem  $k$  choose a measurement outcome  $h_k$  according to the probability distribution

$$\Pr[h_k = w] = |\langle w | U_k^s | j_k \rangle|^2.$$

Fig. 1 presents pseudocode illustrating this method.

### B. Updating the product eigenbasis

In the  $t$ th step of a conventional concordant computation, the unitary gate  $G^t$  is applied to a concordant state  $\rho^{t-1}$  to yield a concordant state  $\rho^t$ . As explained

```

01 Store the unitary operator defining the initial product eigenbasis in  $U$ .
02  $P := I$  (where  $P$  is stored as a sequence of two-bit permutations)
03 For each gate  $G$  in the circuit:
04   If  $G$  has support on only one qubit:
05      $U := GU$ 
06   Else if  $G$  has support on some pair of qubits  $\mathcal{G} = \{k, l\}$ :
07     For each permutation  $Q$  which exchanges two states of the standard basis of part  $\mathcal{G}$ :
08       If  $P^\dagger Q P$  commutes with the initial density operator:
09         The states exchanged by  $Q$  are degenerate. Store this fact.
10       Solve for  $V$ , and thus the new product eigenbasis, using the known degeneracy and the constraint
       that the post-gate state be diagonal in that basis.
11       Pick a permutation  $R$  such that  $VRU^\dagger$  and  $G$  transform the state identically.
12        $P := RP$ 
13        $U := V$ 
14 Output  $P$  and  $U$ .

```

FIG. 2: Pseudocode for converting the sequence of unitary gates in a conventional concordant computation composed of one- and two-qubit gates to an equivalent permutation and change of basis.

in Sec. II C, the effect of  $G^t$  is identical to that of a permutation  $P^t$  of the vectors labeling eigenstates followed by a change of product eigenbasis. Thus, if  $U^{t-1}$  and  $U^t$  are unitary product operators that transform from the standard basis to the product eigenbases at times  $t-1$  and  $t$ , respectively, then  $\rho^t = G^t \rho^{t-1} G^{t\dagger} = U^t P^t U^{t-1\dagger} \rho^{t-1} U^{t-1} P^{t\dagger} U^{t\dagger}$  for some  $P^t$  which permutes the elements of the standard basis. Moreover, Lemma 2 shows that there exists a product eigenbasis for  $\rho^t$  consistent with  $U^t$  such that  $U_k^t = U_k^{t-1}$  for all  $k$  not in  $\mathcal{G}^t$ , the support of  $G^t$ , and additionally, that for such a product eigenbasis there exists a permutation  $P^t$  with support  $\mathcal{G}^t$ .

The problem of finding  $U_k^t$  for  $k \notin \mathcal{G}^t$  is addressed by Lemma 3, which shows that the remaining components of a product eigenbasis for  $\rho^t$  can be calculated given one additional piece of information, the degeneracy of part  $\mathcal{G}^t$  of  $\rho^{t-1}$ . This calculation is efficient in that it entails solving a system of equations whose number depends only on the number of subsystems in  $\mathcal{G}^t$  and their dimension, not on the total number of subsystems in the computation. The appropriate permutation is easily found from the eigenbases for  $\rho^{t-1}$  and  $\rho^t$ ; it is sufficient to pick any permutation mapping eigenprojectors of  $\rho^{t-1}$  to eigenprojectors of  $\rho^t$  which are in the same connected component of a graph  $\Gamma$  defined as per Lemma 2. (Remember that the permutation  $P^t$  can be assumed to have support  $\mathcal{G}^t$ , thereby limiting the size of the graph that must be considered.) As indicated by Theorem 2, these results are sufficient to enable the efficient simulation of concordant computations with most input states. The question of arbitrary input states is taken up in the next section.

**Lemma 3.** For  $\rho = \sum_{\vec{i}} p_{\vec{i}} \mathbb{P}_{\vec{i}}$  and  $\sigma = G \rho G^\dagger$ , where  $G$  is a unitary gate with support  $\mathcal{G}$ ,  $\{\mathbb{Q}^{\vec{j}}\}$  satisfies  $\sigma = \sum_{\vec{j}} \mathbb{Q}_{\vec{j}} \sigma \mathbb{Q}_{\vec{j}}^\dagger$  if and only if  $\text{tr}_{\mathcal{G}}(\rho \mathbb{P}_{\vec{i}}) = \text{tr}_{\mathcal{G}}(\rho \mathbb{P}_{\vec{h}})$  for all  $\vec{h}, \vec{i}$ , and  $\vec{j}$  such that  $G \mathbb{P}_{\vec{h}} G^\dagger \mathbb{Q}_{\vec{j}}^\dagger \neq 0$  and  $G \mathbb{P}_{\vec{i}} G^\dagger \mathbb{Q}_{\vec{j}} \neq 0$ .

*Proof.*

$$\sum_{\vec{i}} G \mathbb{P}_{\vec{i}} G^\dagger \sigma G \mathbb{P}_{\vec{i}} G^\dagger = \sum_{\vec{i}} G \mathbb{P}_{\vec{i}} \rho \mathbb{P}_{\vec{i}} G^\dagger = G \rho G^\dagger = \sigma,$$

so by Lemma 1,  $\{\mathbb{Q}^{\vec{j}}\}$  satisfies  $\sigma = \sum_{\vec{j}} \mathbb{Q}_{\vec{j}} \sigma \mathbb{Q}_{\vec{j}}^\dagger$  if and only if  $\text{tr}_{\mathcal{G}}(\sigma G \mathbb{P}_{\vec{h}} G^\dagger) = \text{tr}_{\mathcal{G}}(\sigma \mathbb{Q}_{\vec{j}})$  for all  $G \mathbb{P}_{\vec{h}} G^\dagger \mathbb{Q}_{\vec{j}}^\dagger \neq 0$ . Given  $\rho, \sigma, G, \{\mathbb{P}_{\vec{i}}\}$ , and  $\{\mathbb{Q}^{\vec{j}}\}$  as defined, the condition  $\text{tr}_{\mathcal{G}}(\sigma G \mathbb{P}_{\vec{h}} G^\dagger) = \text{tr}_{\mathcal{G}}(\sigma \mathbb{Q}_{\vec{j}})$  for all  $G \mathbb{P}_{\vec{h}} G^\dagger \mathbb{Q}_{\vec{j}}^\dagger \neq 0$  is equivalent to  $\text{tr}_{\mathcal{G}}(\rho \mathbb{P}_{\vec{h}}) = \text{tr}_{\mathcal{G}}(\rho \mathbb{P}_{\vec{i}})$  for all  $G \mathbb{P}_{\vec{h}} G^\dagger \mathbb{Q}_{\vec{j}}^\dagger \neq 0$  and  $G \mathbb{P}_{\vec{i}} G^\dagger \mathbb{Q}_{\vec{j}} \neq 0$ .  $\square$

Fig. 2 presents pseudocode for an algorithm calculating the necessary sequence of permutations and basis changes.

**Theorem 2.** A conventional concordant computation with an input product state that is generic can be efficiently simulated by a classical computer.

*Proof.* A generic product state has no degenerate eigenvalues, so the simulation method as outlined thus far is sufficient for such input states.  $\square$

### C. Diagnosing the degeneracy

In order to update the product eigenbasis following the  $t$ th gate in a conventional concordant computation, it is necessary to diagnose the degeneracy of part  $\mathcal{G}^t$  of  $\rho^{t-1}$ , where  $\mathcal{G}^t$  is the support of  $G^t$ , the  $t$ th gate in the computation, and  $\rho^{t-1}$  is the state of the computation at time  $t-1$ . This degeneracy can be found by determining whether  $\rho^{t-1}$  and  $U^{t-1} Q U^{t-1\dagger}$  commute for each permutation  $Q$  exchanging two eigenstates of the standard basis for the subsystems in  $\mathcal{G}^t$ . As the simulation algorithm progresses, permutations equivalent to

each gate are found, so  $\rho^{t-1} = U^{t-1} P \rho^0 P^\dagger U^{t-1\dagger}$  where  $P = \prod_{r=1}^{t-1} P^r$  represents the sequence of (known) permutations up to step  $t-1$ . Thus, one may equally well check whether

$$\rho^0 = P^\dagger Q P \rho^0 P^\dagger Q P. \quad (9)$$

I now restrict my attention to concordant computations composed of two-qubit gates acting on a register of  $n$  qubits. The permutation  $P^\dagger Q P$  is an involution, i.e., it is self-inverse, and for the case of qubits and two-qubit gates, it is affine when considered as a function on binary vectors. Lemma 4 shows that such a permutation commutes with  $\rho^0$  if and only if Eq. 9 is satisfied for the pure product state corresponding to each of a particular set of  $n+1$  binary vectors. Consequently, the commutativity of  $\rho^0$  and  $P^\dagger Q P$ , and therefore the degeneracy relevant to updating the product eigenbasis, can be efficiently determined for concordant computations composed of two-qubit gates.

**Lemma 4.** *A product state on qubits,  $\rho = \bigotimes_k \rho_k$ , such that  $\rho$  is diagonal in the standard basis and  $e_k = \langle 1 | \rho_k | 1 \rangle / \langle 0 | \rho_k | 0 \rangle \leq 1$  for all  $k$  commutes with an affine involution  $S$  if and only if  $\langle \vec{i} | S \rho S^\dagger - \rho | \vec{i} \rangle = 0$  for all  $|\vec{i}\rangle$  such that  $i_k = \delta_{kl}$  or  $i_k = 0$ .*

*Proof.*

Throughout this proof, binary vectors labeling states are represented by the set of indices identifying bits in the  $|1\rangle$  state. Let  $\mathcal{S}$  be a version of  $S$  that acts on such sets<sup>2</sup>. In this representation, the affine linearity of  $S$  is expressed as  $\mathcal{S}(\mathcal{A} \ominus \mathcal{B}) = \mathcal{S}(\mathcal{A}) \ominus \mathcal{S}(\mathcal{B}) \ominus \mathcal{K}$  for some fixed  $\mathcal{K}$ , while the fact that  $S$  is an involution implies that  $\mathcal{S}(\mathcal{S}(\mathcal{A})) = \mathcal{A}$ . Define  $\mathcal{C}_e = \{k : e_k = e\}$  and  $f(\mathcal{B}) = \prod_{k \in \mathcal{B}} e_k$ . In terms of  $f$  and  $\mathcal{S}$  the commutativity condition to be satisfied is

$$f(\mathcal{B}) = f(\mathcal{S}(\mathcal{B})) \quad (10)$$

for any set of bits,  $\mathcal{B}$ .

The forward implication stated in this lemma is trivial. If Eq. 10 is satisfied for any set  $\mathcal{B}$  then it is obviously satisfied for any singleton  $\{k\}$  and for the empty set.

To demonstrate the reverse, I assume, for the remainder of the proof, that Eq. 10 is satisfied for the empty set and any singleton and seek to show that it is satisfied in general. I organize what follows in terms of a sequence of small points.

**Point 0:**  $\mathcal{T}(\mathcal{B}) = \mathcal{S}(\mathcal{B}) \ominus \mathcal{K}$  is a linear involution, and  $\mathcal{T}$  satisfies Eq. 11 if and only if  $\mathcal{S}$  satisfies Eq. 10.  $\mathcal{T}$  is linear since  $\mathcal{S}$  is affine with constant  $\mathcal{K}$ . Because

$\mathcal{S}(\emptyset) = \mathcal{K}$  and  $\mathcal{S}$  is an involution,  $\mathcal{S}(\mathcal{K}) = \mathcal{S}(\mathcal{S}(\emptyset)) = \emptyset$ , implying that  $\mathcal{T}$  is an involution since

$$\begin{aligned} \mathcal{T}(\mathcal{T}(\mathcal{B})) &= \mathcal{T}(\mathcal{S}(\mathcal{B}) \ominus \mathcal{K}) = \mathcal{S}(\mathcal{S}(\mathcal{B}) \ominus \mathcal{K}) \ominus \mathcal{K} \\ &= \mathcal{S}(\mathcal{S}(\mathcal{B})) \ominus \mathcal{S}(\mathcal{K}) \ominus \mathcal{K} \ominus \mathcal{K} = \mathcal{B}. \end{aligned}$$

Furthermore,  $\mathcal{K} \subseteq \mathcal{C}_1$  since if  $\exists k \in \mathcal{K}$  such that  $k \notin \mathcal{C}_1$  then  $f(\mathcal{K}) \leq e_k < 1 = f(\emptyset)$ . Consequently,  $f(\mathcal{B}) = f(\mathcal{B} \ominus \mathcal{K})$ , and thus Eq. 10 is satisfied if and only if

$$f(\mathcal{B}) = f(\mathcal{T}(\mathcal{B})) \quad (11)$$

**Point 1:**  $\forall k \exists m \in \mathcal{T}(k)$  such that  $k \in \mathcal{T}(m)$ . Because  $\mathcal{T}$  is a linear involution,

$$k = \mathcal{T}(\mathcal{T}(k)) = \mathcal{T}\left(\bigoplus_{l \in \mathcal{T}(k)} \{l\}\right) = \bigoplus_{l \in \mathcal{T}(k)} \mathcal{T}(l),$$

so  $\forall k \exists m \in \mathcal{T}(k)$  such that  $k \in \mathcal{T}(m)$ .

**Point 2:**  $e_l \geq e_k \forall l \in \mathcal{T}(k)$

If  $\exists l \in \mathcal{T}(k)$  such that  $e_l < e_k$  then  $f(k) = e_k > e_l \geq f(\mathcal{T}(k))$ , so  $e_l \geq e_k \forall l \in \mathcal{T}(k)$ .

**Point 3:**  $\exists m \in \mathcal{T}(k)$  such that  $e_m = e_k$

By the previous two points  $\exists m \in \mathcal{T}(k)$  such that  $k \in \mathcal{T}(m)$  and  $e_m \geq e_k$ , but this implies that  $e_m = e_k$  since, by Point 2,  $k \in \mathcal{T}(m)$  implies  $e_k \geq e_m$ .

**Point 4:** Each  $k \in \mathcal{C}_e$  where  $e > 0$  is mapped by  $\mathcal{T}$  to a single  $m \in \mathcal{C}_e$  together with (possibly) some elements of  $\mathcal{C}_1$ .

By the previous point,  $\exists m \in \mathcal{T}(k)$  such that  $m \in \mathcal{C}_{e_k}$ , implying that

$$f(\mathcal{T}(k)) = f(m)f(\mathcal{T}(k) \setminus \{m\}) = e_k \prod_{l \in \mathcal{T}(k) \setminus \{m\}} e_l,$$

which is equal to  $f(k) = e_k$  only when  $e_k = 0$  or  $e_l = 1 \forall l \in \mathcal{T}(k) \setminus \{m\}$ .

**Point 5:** Any two distinct elements  $k, l \in \mathcal{C}_e$  where  $e > 0$  are mapped by  $\mathcal{T}$  to distinct elements of  $\mathcal{C}_e$  together with (possibly) some elements of  $\mathcal{C}_1$ .

If  $\exists k, l \in \mathcal{C}_e$  with  $k \neq l$  and  $1 > e > 0$  such that  $\mathcal{T}(k)/\mathcal{C}_1 = \mathcal{T}(l)/\mathcal{C}_1 = \{m\}$  then  $k, l \in \mathcal{T}(m)$  since  $k, l \notin \mathcal{T}(o)$  for any  $o \in \mathcal{C}_1$ , which contradicts the preceding point.

**Point 6:** If  $\mathcal{B} \cap \mathcal{C}_0 \neq \emptyset$  then  $\mathcal{T}(\mathcal{B}) \cap \mathcal{C}_0 \neq \emptyset$ .

If  $\exists \mathcal{B}$  such that  $\mathcal{B} \cap \mathcal{C}_0 \neq \emptyset$  but  $\mathcal{T}(\mathcal{B}) \cap \mathcal{C}_0 = \emptyset$  then  $\exists l \in \mathcal{T}(\mathcal{B})$  such that  $e_l > 0$  and  $\mathcal{T}(l) \cap \mathcal{C}_0 \neq \emptyset$ , which contradicts my second point.

**Point 7:** Eq. 11 is satisfied for any set  $\mathcal{B}$ .

If  $\mathcal{B} \cap \mathcal{C}_0 \neq \emptyset$  then  $\mathcal{T}(\mathcal{B}) \cap \mathcal{C}_0 \neq \emptyset$  so  $f(\mathcal{B}) = f(\mathcal{T}(\mathcal{B})) = 0$ .

<sup>2</sup> For brevity I omit brackets in the argument of this and other functions when the input is a singleton, e.g., I write  $\mathcal{S}(k)$  rather than  $\mathcal{S}(\{k\})$ .

Otherwise,

$$\begin{aligned} f(\mathcal{B}) &= \prod_{l \in \mathcal{B}} f(l) = \prod_{l \in \mathcal{B}} f(\mathcal{T}(l)) = f\left(\bigoplus_{l \in \mathcal{B}} \mathcal{T}(l)\right) \\ &= f\left(\mathcal{T}\left(\bigoplus_{l \in \mathcal{B}} \{l\}\right)\right) = f(\mathcal{T}(\mathcal{B})), \end{aligned}$$

where the middle equality follows from Point 5, which shows that  $\mathcal{T}(l) \cap \mathcal{T}(k) \subseteq \mathcal{C}_1$  for all  $k$  and  $l$  such that  $k \neq l$  and  $k, l \notin \mathcal{C}_0, \mathcal{C}_1$ .  $\square$

#### IV. EXTENSIONS

Quantum computations, even those described in terms of quantum circuits, frequently are not envisioned in the conventional form outlined by Def. 4. The most common deviations are the inclusion of single-subsystem measurements intermixed with the unitary operators and the introduction of new subsystems during the course of the computation. Another possibility for concordant computations is that the input state be a mixture of product states that is not also a product of mixed states but that can be efficiently prepared due to the mixture having few terms. Computations with these features can be converted to conventional ones (allowing for some post selection to assist in the generation of the desired input state), but, in general, the conversion process preserves neither the concordance of the computation nor the maximal support of its unitary operators. While subsystems introduced during the course of a computation can equally well be introduced at its beginning, non-terminal measurements and non-product-state inputs require special treatment.

##### A. Non-terminal measurements

It requires some effort to extend the simulation algorithm described in the previous section to non-terminal measurements on single subsystems. Through the first measurement, the simulation may proceed exactly as previously explained, but subsequent to that, a more complex technique for diagnosing the degeneracy is necessary since measurements introduce the possibility that the degeneracy relevant to determining the permutation and change of eigenbasis equivalent to a gate might be dependent on the outcome of the measurement result. There seems to be a method of efficiently diagnosing the relevant degeneracy when measurements are performed in the eigenbasis, but the more general problem is one that I have not yet been able to solve.

##### B. Non-product-state inputs

Generically, Def. 4 excludes a very natural kind of mixed input state, namely, the probabilistic mixture of a few pure product states. As it happens, however, concordant computations with such input states are easy to simulate; the state of the computer can simply be stored and updated explicitly. The algorithm is the same as that described in Sec. III except that the degeneracy is straightforward to evaluate since the state is explicitly known. Because unitary operators do not change the rank of density matrix and projective measurements can only decrease it, explicit storage of the state remains practical throughout the simulation.

Effectively, a quantum computation on a low-rank input state becomes complicated only because the eigenbasis becomes complicated. For a concordant computation the eigenbasis remains manageable.

#### V. CONCLUSION

In summary, I have shown that conventional concordant computations composed exclusively of gates acting on one or two qubits can be efficiently simulated using a classical computer. As a consequence, such a computation must generate quantum discord if it is to permit the efficient solution of a problem requiring super-polynomial resources classically. A similar statement holds for more general gate sets whenever the input state is either a generic product state or a mixture of a few pure product states. These results lend support to the idea that quantum discord is the appropriate generalization of entanglement with regard to mixed-state quantum computation. That being said, concordance is such a stringent property that it no doubt corresponds to the case of zero quantum correlations for a variety of measures (including the many flavors of discord), so this is far from the final word on the subject. As has periodically been noted, it is also important to keep in mind that there can be no single resource for quantum computing; If quantum computations without property  $\mathcal{P}$  can be efficiently simulated classically then  $\mathcal{P}$  is a necessary resource for achieving a Promethean speedup.

Several possible directions for future research are suggested by previous work on simulating quantum computations with restricted entanglement. The two most prominent are investigating the performance of the simulation for approximately concordant states and extending it to computations where discord is restricted to blocks of qubits of bounded size. A block of qubits with unrestricted correlations can be treated as a single quantum system, so progress on the latter topic would likely require extending the simulation method to qudits.

Though I specialize to qubits and two-qubit gates only in Sec. III C, it is doubtful whether my simulation method can be extended to more general gate sets. Section III C depends crucially on the fact that permutations on one or



two bits of a vector are necessarily linear (or, from an alternate perspective, that such permutations are Clifford gates) since this allows me to determine whether Eq. 9 is satisfied by checking a small set of basis vectors. On the other hand, permutations on systems of dimension greater than two or on more than two bits need not be linear. Thus, directly generalizing the method of simulation described in this paper requires a means of testing Eq. 9 for an arbitrary sequence of permutations and input (mixed) product state. This implies the ability to efficiently solve 3-SAT, an NP-Complete problem, since  $P$  in Eq. 9 can be chosen to implement a boolean formula,  $Q$  to copy the result to an ancillary qubit, and  $\rho^0$  to consist of unbiased input qubits and maximally biased ancillary qubits, yielding  $\rho^0 \neq P^\dagger Q P \rho^0 P^\dagger Q P$  if and only

if the boolean formula is satisfied for some input. In other words, a direct extension of my simulation method is effectively ruled out, though I am unable to exclude the possibility that some more generally applicable method exists for simulating concordant computations.

### Acknowledgments

I am grateful to Emanuel Knill, Anil Shaji, Carlton Caves, Vaibhav Madhok, and Adam Meier for many productive discussions. This paper is a contribution by the National Institute of Standards and Technology and, as such, is not subject to U.S. copyright.

- 
- [1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Rev. Mod. Phys.* **81**, 865 (2009), [arXiv:quant-ph/0702225](#).
  - [2] R. Jozsa and N. Linden, *Proc. R. Soc. A* **459**, 2011 (2003), [arXiv:quant-ph/0201143](#).
  - [3] G. Vidal, *Phys. Rev. Lett.* **91**, 147902 (2003), [arXiv:quant-ph/0301063](#).
  - [4] R. Orús and J. I. Latorre, *Phys. Rev. A* **69**, 052308 (2004), [arXiv:quant-ph/0311017](#).
  - [5] E. Knill and R. Laflamme, *Phys. Rev. Lett.* **81**, 5672 (1998), [arXiv:quant-ph/9802037](#).
  - [6] L. S. A. Ambainis and U. Vazirani, *Journal of the ACM* **53**, 507 (2006), [arXiv:quant-ph/0003136](#).
  - [7] A. Datta, S. T. Flammia, and C. M. Caves, *Phys. Rev. A* **72**, 042316 (2005), [arXiv:quant-ph/0505213](#).
  - [8] A. Datta and G. Vidal, *Phys. Rev. A* **75**, 042310 (2007), [arXiv:quant-ph/0611157](#).
  - [9] W. H. Zurek, *Ann. Phys.* **9**, 855 (2000), [arXiv:quant-ph/0011039](#).
  - [10] A. Datta, A. Shaji, and C. M. Caves, *Physical Review Letters* **100**, 050502 (2008), [arXiv:0709.0548](#).
  - [11] B. P. Lanyon, M. Barbieri, M. P. Almeida, and A. G. White, *Phys. Rev. Lett.* **101**, 200501 (2008), [arXiv:0807.0668](#).
  - [12] H. Ollivier and W. H. Zurek, *Phys. Rev. Lett.* **88**, 017901 (2001), [arXiv:quant-ph/0105072](#).